Technical Note

1965-3

J. B. Connolly
W. G. Schmidt

Failure Erasure Circuitry:
A Duplicate Technique
for Failure-Masking Systems

14 October 1965

Lincoln Laboratory

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Lexington, Massachusetts

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

LINCOLN LABORATORY

FAILURE ERASURE CIRCUITRY:
A DUPLICATE TECHNIQUE FOR FAILURE-MASKING SYSTEMS

J. B. CONNOLLY
W. G. SCHMIDT

Group 63

TECHNICAL NOTE 1965-3

14 OCTOBER 1965

LEXINGTON   MASSACHUSETTS

ABSTRACT

There are generally considered to be four major types of digital circuit redundancy techniques in use today. They are the Shannon-Moore component redundancy method, the "quadded logic" approach suggested by Tryon, von Neumann's triplication and majority-voting technique, and the basic standby redundancy systems. When viewed in the light of design criteria which are based upon the requirements of non-maintainable spacecraft, it appears that the triplication and majority-voting scheme is optimal, although more costly in weight, power, and component cost than one would prefer. It is the purpose of this paper to describe a redundancy technique which would require mere duplication to achieve the same failure-masking capabilities as the von Neumann method.

An analysis of the circuit-failure problem is approached from the viewpoint of coding theory with comparisons made between the "noisy channel" and "circuit-failure" problems. Some of the difficulties of extrapolating from the former to the latter are discussed, as well as recent attempts to minimize the redundancy "overhead" by coding over larger numbers of bits.

Following a description of the binary erasure channel model, a proposal of a failure-erasure technique based upon it is outlined. The method enables failure-masking at duplicative rather than triplicative costs. There are constraints which this scheme imposes upon the circuit elements, however, and the characteristics of the ideal circuit element and logic signaling are proposed. The paper concludes with a discussion of existing hardware which approximates the desired characteristics.

TABLE OF CONTENTS

INTRODUCTION

Foremost among the requirements for electronics of the future is the ability of these systems to perform reliably for exceptionally long periods of time without need for maintenance of any sort. Pioneering efforts in this direction were made primarily in the submarine cable area but it was only with the advent of complex airborne electronic systems that terms like "quality control", "maintainability" and "MTBF" made their appearance in the technical literature. The demands which non-maintainable space-borne electronics systems have made upon component test and evaluation and associated areas have forced electronic components to reach very high levels of reliability.

The fact remains, nevertheless, that while components are more reliable than ever, the increasing complexity of space-borne electronics, coupled to the need for exceptionally long operating lifetimes of five to ten years, leaves little hope for reliable components alone to achieve the desired goals. There is always the finite probability that the first failure will occur much more quickly than the anticipated mean time. When one has to design an exceptionally reliable system this possibility must always be considered and the cost of the addition of failure-masking techniques (perhaps just in critical areas) should be considered. There are drawbacks to the use of redundancy also, particularly in terms of additional weight and power. It is the purpose of this paper to propose a redundancy technique which will reduce the traditional redundancy "overhead" by about fifty per cent.

EXISTING REDUNDANCY TECHNIQUES

Before entering into a discussion of the analog of communications channels in failure-masking techniques, it might be well to review what the authors consider the major contemporary techniques currently being employed to one extent or another. The four schemes to be reviewed are discussed in more detail elsewhere[1] and, accordingly, only brief descriptions will be given in this paper.

---

[1] An excellent single source of information on redundancy schemes is "Redundancy Techniques for Computing Systems" edited by Wilcox and Mann, Spartan Books, 1962.

The first redundancy technique to be considered is normally applied at the component level and is probably the redundancy method most used today. Called the Shannon-Moore scheme,[2] it relies upon knowing the probability of a particular failure mode (open or short circuit). In the extreme case where a component will only fail in a short circuit mode, the redundant configuration of Figure 1a should be used. Where the component will only fail as an open circuit, the configuration of Figure 1b is an obvious choice. Figure 1c is used for a component whose short-failure probability is equal to its open-failure probability. The original paper referred to redundant relays, which were open or closed, by design or otherwise. The use of this technique for other types of components must be very carefully considered in order to preserve the basic tenet of this, and any other redundancy scheme, which is the statistical independence of the failures. This technique may be used in linear circuitry also but also must be applied with caution. A failure occurring within a redundant set should not increase the stress level on the other components within the set. A difficulty with this system, and most component redundancy schemes above and beyond that of power and weight increases, is that of determining where failures exist prior to the equipment entering its critical non-maintainable period of operation. Component redundancy makes this somewhat difficult to achieve. Some schemes have been employed in which the redundant configurations are split into two distinct systems which are independently tested and, upon successful completion of these tests, the two systems are reconnected into one. Such techniques generally do not, however, verify that all components are working. The increased usage of integrated circuitry, some types of which display a relative lack of isolation between circuit elements, may further limit the use of this scheme. The component cost of this technique is generally about a factor of four above that of the non-redundant scheme. As components fail, power consumption increases. Because of the change in the equivalent component

---

[2]Moore, E. F. and C. E. Shannon, "Reliable Circuits Using Less Reliable Relays", Journal of the Franklin Institute, 1956.

impedance as failures occur, it is not prudent to use such methods where component values must be precisely controlled.

Another scheme for failure-masking is called "quadded logic" or Tryon's method,[3] this technique operates best at the circuit level. It is based upon quadruplication of circuitry and the error is usually corrected within two or three levels of logic "downstream" from the initial failure. Correction is based upon receiving correct signals from the previous levels, which are interwoven in connection networks to minimize propagation of the error. Boolean expressions which contain "don't care" terms actually do the correction. For example

$$1 + \underline{0} = 1 + \underline{1} = 1$$
$$0 \times \underline{1} = 0 \times \underline{0} = 0$$

where

the underlined term is the "don't care" or "correctable" term for that particular expression. A logical network is shown in Figure 2a and its quadded equivalent is shown in Figure 2b.

There are a number of disadvantages to this technique, not the least of which is the quadruplication of circuits and the interconnection morass, which begets unreliability. Power consumption is quadrupled also. The debugging of such a system is very difficult and on a par with the Shannon-Moore scheme. The use of this method for timing circuitry such as astable or monostable multivibrators, is also troublesome.

The third major method of implementing redundant systems is the majority-voting scheme originally proposed by von Neumann.[4] The technique involves

---

[3]Tryon, J. G., "Quadded Logic" in Wilcox and Mann, op. cit. p. 205.

[4]von Neumann, J., "Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components", Automata Studies, Annals of Mathematics Studies, No. 34. Princeton University Press, 1956.

3

triplication, at least, with restoration of the desired signal accomplished through a "restorer" which is a majority-voting logic element. This type of redundancy is usually applied at a subsystem or systems level and is shown in a block diagram in Figure 3a. In order to guard against a failure of the voting circuit, a redundant system, using this method, may be arranged as shown in Figure 3b.

From the standpoint of prelaunch debugging, this method offers the greatest advantage since the system may be trisected into three non-redundant systems, a failure in which is readily detectable. After debugging, the portions are reconnected. The power and weight dissipated in such a system are multiplied by a factor which is slightly greater than three. The circuitry used may be of the conventional variety and commercially available integrated circuits may be employed. Free-running timing circuitry still presents problems in this scheme. Care must also be taken in turning on such a system since certain subsystem circuitry, such as counters, must have the same starting point. Since a transient noise condition can make a counter disagree with its two redundant counters (triplication is assumed), the use of feedback of the restored signal might be employed to obtain correction of the transient-induced miscounting. Feedback shift registers may be used as counters to advantage under these circumstances, as shown in Figure 4.

An interesting variation of the straightforward majority-voting scheme has been proposed by W. H. Pierce[5] and is based upon adaptive weighting of the signals entering the signal restorer, or vote-taker.

The final redundancy scheme, "standby" redundancy, is perhaps the most basic. In this method a system is operated with one or more identical systems kept in parallel but not operating. When the operating system is detected as

[5] Pierce, W. H., "Adaptive Vote-Takers Improve the Use of Redundancy", Redundancy Techniques for Computing Systems. op. cit.

being in error or as having failed, a signal is generated which turns on the next "standby" system. The difficulty with this arrangement is the detection of the error, or failed system, with a minimum number of available operating systems. More will be mentioned of this problem shortly but, suffice to say at this time, this is a rather complex problem involving minimum redundancy design. However, if the failure mode to be masked is comparatively simple, this technique can be used effectively.

To conclude this review of the major redundancy schemes, it appears that on the basis of ease of prelaunch checkout and minimum numbers of components, that the triplication and majority-voter technique is the most feasible although there are areas within a digital system, such as time base generators, where one would find another approach more practical. The power and weight penalty is a factor slightly more than three. It appears to be of significant advantage if a minimum-redundancy scheme could be evolved which would allow much smaller "overhead" for failure-masking systems.

COMMUNICATION CHANNEL ANALOGS

In this section, suggestions deriving from coding and communication theory as tools to generate redundant digital systems are discussed. The approach taken is to discuss the traditional usage of coding theory in the transmission of digital information, then to show the differences between such traditional usage and the problem at hand. It is seen that the type of failure considered here, catastrophic circuit failure, is handled only by the paralleling of circuits. An example of the use of coding theory to determine the optimum degree of parallelism is given and the limitations discussed. An alternate technique based on the erasure channel is then developed.

A block diagram of a simple digital communications system is shown in Figure 5. This system consists of the series connection of an information source, an encoder, a transmitter, a channel, a receiver, a decoder, and an information user. Typically the information source supplies messages in

5

binary form; also it is generally assumed that as signals propagate through the channel they are corrupted or perturbed by some kind of noise. The encoder-decoder operate as a pair so that the binary messages can be transmitted from information source to information user with the least probability of error.

The usual problem associated with such digital systems is the design of the encoder-decoder. Although coding techniques have been developed for a perfectly noiseless channel the major emphasis has always been on systems in which the channel had noise characteristics. In particular, it is the purpose of these codes to detect and sometimes to detect and correct such errors.[6] Generally these codes require that the occurrence of errors be independent of digit position. This is statistical independence of errors. Certain other codes have been developed which will correct bursts of errors in a message. In fact, a fundamental theorem of coding tells us that it is possible to encode and to decode in such a fashion that (consistent with the channel capacity) the probability of incorrect decoding can be made arbitrarily small.[7] Unfortunately, no straightforward design path for the realization of this exists. Typical coding techniques exchange error correction capability for rate of information transmission.

The block diagram of Figure 5 shows a series connection which, as mentioned previously, is typical. There are many different sources of noise which can perturb the signals in the channel. Notwithstanding the noise source itself, the principal effect of the noise, signal corruption, is relatively transient. That is one does not find message after message completely incorrect (prior to decoding) rather one finds errors here and there, scattered throughout the word length. Completely incorrect messages would be

---

[6] Peterson, W. W., "Error-Correcting Codes", M.I.T. Press and John Wiley & Sons, 1961.

[7] Shannon, C. E., "The Mathematical Theory of Communication", BSTJ, pp. 379-423; 1948.

indicative of a catastrophic failure in the series connection. No amount of coding dexterity will correct the errors due to such a catastrophic failure in a series connection.

It is seen therefore, that codes can be effective against transient type noise in a series connected system but that they are useless against catastrophic failures.

In most digital systems the noise perturbing the channel is generally not excessive due to the fact that the channel may be simply a wire connection running a distance of several feet. The primary cause of error is the failure of circuits. Circuit failure can be transient in nature, due to component and power supply drift, poor interconnections causing intermittent failure, and the like. Even with the series connection, as long as the transient errors are truly transient, then the use of codes would be beneficial.

On the other hand, circuit failure can be catastrophic with the net result that the series information flow chain is permanently broken. These failures can come about from extreme voltage and component variation, opens and shorts, and so forth. Coding cannot help here when a series connection is used.

If it is desired to correct errors due to catastrophic circuit failures, then it is clear that the series connection of elements is useless and some kind of parallel arrangement is required. Various kinds of parallel arrangements were discussed in previous sections; these parallel configurations differ in degree of parallelism in the sense of the amount of extra hardware, space, power consumption, and cost. Error correction techniques in the form of coding can help to determine an optimum degree of parallelism.

It is extremely important to realize that at this point we have shifted our attention from the use of coding to generate time redundancy to the use of coding to generate parallel redundancy because of the inherent differences between the failure modes. Consider a circuit, as shown in Figure 6, consist-

7

ing of a Boolean function element and parity operators. If a Hamming single error correcting code is used, then a word three digits long can be used with positions 1 and 2 containing the parity digits for the information digit in position 3.
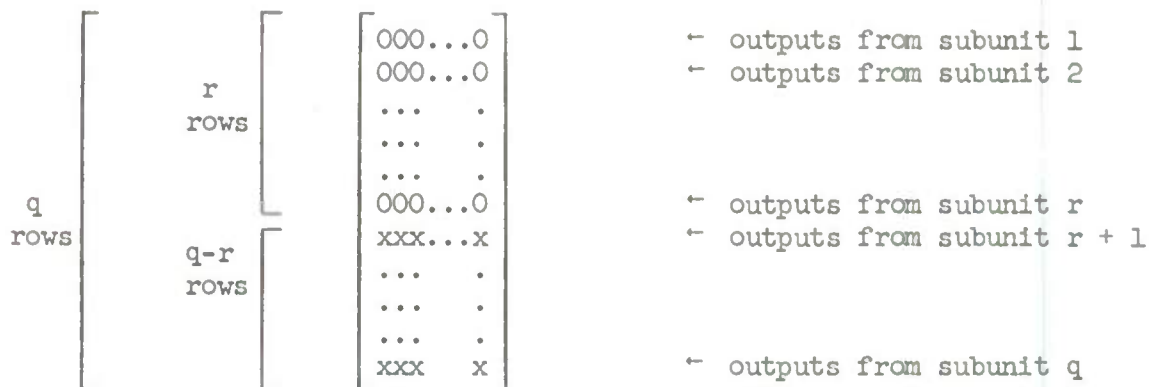
The classical coding approach would be to determine the position of the incorrect bit through the parity check equations. The correction would be accomplished by complementing the bit in the position indicated. Some thought about this reveals that a non-trivial amount of logic is required to perform the implementation.

However, if words 000 and 111 are chosen, corresponding to the information digit, being 0 and 1 respectively, it can readily be verified that the parity operators are the same as the function element shown in Figure 7. If the majority vote taker is used as a decoder, as shown in Figure 8, then the implementation of error correction can readily be carried out. It is desirable to retain the parity check to detect an error since the majority vote taker automatically carries out the correction, thus masking the fact that an error occurred.

A similar technique was previously considered by Armstrong[8] who carried it further to attempt to take advantage of the fact that as the number of information digits per message grows, then the ratio of check digits to information digits goes down. Armstrong's arguments concern a digital system with m inputs and n outputs. It must be such that it can be broken down into r electrically independent subunits, each subunit carrying not more than p of the n outputs. The diagram is shown in Figure 9. Consider the following matrix, in which the outputs of each subunit are displayed in a separate row with p entries per row. The (q-r) additional subunits provide the necessary check digits.

8

Armstrong, D. B., "A General Method of Applying Error Correction to Synchronous Digital Systems", BSTJ, pp. 577-593; March 1961.

$$\left[\begin{array}{c} \left[\begin{array}{c} r \\ rows \end{array} \right. \\ \\ \\ \left. \begin{array}{c} q-r \\ rows \end{array} \right. \end{array} \right. q\ rows \left[\begin{array}{l} 000\ldots0 \\ 000\ldots0 \\ \cdots\quad\cdot \\ \cdots\quad\cdot \\ \cdots\quad\cdot \\ 000\ldots0 \\ xxx\ldots x \\ \cdots\quad\cdot \\ \cdots\quad\cdot \\ \cdots\quad\cdot \\ xxx\quad x \end{array} \right]$$

$\leftarrow$ outputs from subunit 1
$\leftarrow$ outputs from subunit 2

$\leftarrow$ outputs from subunit r
$\leftarrow$ outputs from subunit r + 1

$\leftarrow$ outputs from subunit q

If the error to be corrected is assumed to occur in only one subunit, then at most a single row can have errors. Hamming single error correcting codes can be used with each column regarded as a message word. It is clear that the cost of redundancy can be made much less than for the triplication scheme. Ray-Chaudhuri has shown that since the errors can occur only along a single row, that is, the error position in each word must be common to all words, then codes which require fewer parity bits for the same message length than Hamming codes are feasible.[9]

The equipment redundancy is essentially created by the parity check circuits and the error correcting circuits. The error correcting circuits, as noted previously, are quite difficult to realize and it is here that certain of the advantages gained by coding are offset. Armstrong's estimate of the total equipment redundancy is a factor of three for most systems. A simple example of the technique is shown in Figure 10. The objective is to select one of $(xy, x'y, x'y', xy')$ given (x, x', y, y').

The nonredundant logic requires four AND gates and the generation of the three parity bits requires three OR gates. In this case the redundancy introduced is less than the original system. Minimization of the error correction logic will, however, significantly increase the overhead. It should be clear that coding theory can lead the way to a rigorous determina-

_____

[9] Ray-Chaudhuri, D., "On the Construction of Minimally Redundant Reliable System Designs". BSTJ, pp. 595-611; March 1961.

tion of the optimum degree of circuit parellelism but to date even the most sophisticated schemes are expensive and cumbersome primarily due to the complexity of the decoding and error correction mechanism.

It is felt that it should be possible to translate certain other communication theory ideas into digital circuit design specifications such that the degree of total equipment redundancy can be made lower.

Consider a binary erasure channel (BEC) as shown in Figure 11. The channel diagram shows that if a 0 is transmitted it will either be received as a 0 with probability p or received as a no decision (equivalent to "I don't know whether the bit sent was 0 or 1") with probability q. Similar remarks apply to a 1 being transmitted.

Suppose that one had available digital circuits such that a model for their operation would be similar to the BEC. These circuits would have specified failure modes which would be equivalent to the no decision node of the BEC. In this case a simple duplication of the original circuit and the addition of an OR circuit can correct any single error provided that the failure modes are such that the OR circuits are insensitive to them. A diagram of such a system is shown in Figure 12. The model for the operation of either the A or the B system, shown in Figure 13, indicates that the system has n inputs or 2^n distinct input states. When the system operates correctly each input state has a correct output state which is either 0 or 1 depending on the particular input state and the logical function of the system. In addition, every input state has a path to a no decision state. The truth table for the OR circuit is shown below.

A (output)	B (output)	OR (output)
0	0	0
1	1	1
ND	0	0
ND	1	1
0	ND	0
1	ND	1
ND	ND	ND

The OR element operational model is shown in Figure 14. This model implements the truth table and illustrates the operating philosophy of the binary erasure channel as applied to the enhancement of the reliability of operating digital systems. In an operational configuration, the circuit elements would be disposed as shown in Figure 15, in order that the two distinct systems may be separated for individual checkout. With each OR circuit receiving but one signal and a "no decision" from the unconnected input wire, the individual sections should still work perfectly.

The actual design of electronic circuits possessing the characteristics specified here will be considered in the following section.

THE DESIGN OF FAILURE-ERASURE CIRCUITRY

The basic requirement of failure-erasure circuitry is that any abnormal component parameter drift or catastrophic failure have an immediate influence upon the transfer characteristics of that logic network such that the subsequent logic elements will not respond to the output signals of the faulty element. In the failure-masking system, the OR "decoder" must not malfunction if one of the inputs carries a "no decision" signal.

There are then several characteristics which must be designed into failure-erasure circuitry; a high degree of inter-component dependence leading to tight control over the output characteristics is essential, knowledge of the failure-modes of the components within the networks is vital as is the use of output signals which are less likely to be misconstrued in decoding. The relative isolation achievable between duplicated networks must be high so that a failure of one network does not interact with the duplicated network. The reliability of the decoder must be exceptional.

Let us now look into these characteristics in further detail and attempt to synthesize the type of logical element desired. The most formidable of the desired features is the ability of any component failure, catastrophic or

11

severe drift, within the network to drastically influence the network output in such a way as to yield the ND signal, or any signal which is obviously not a "1" or "0". It would appear that the most feasible logical element, as well as the most reliable one, is one that has a minimum of components. For example, in a simple parallel RLC circuit an open resistor would make itself known by an increase in output amplitude and a catastrophic short in the capacitor would put an abrupt end to the oscillation of the tank. As one departs from the three-parameter network into more complex networks, the contribution of each component becomes increasingly masked by the peripheral components until a single component failure in a network may scarcely influence the form of the output signals of that network but may still yield faulty information. Indeed, since most logic circuitry employs transistors used as switches, a transistor which fails catastrophically as an open or a short will yield an output signal which is identical to one of its operational output signals.

This point might be enlarged upon to stress the fact that linear logic signals, by reason of their higher information content, are more amenable to failure detection techniques. The classical input-output characteristics of the digital gate, usually with a saturating active element used as an inverter, would look like Figure 16, with the normal operating tolerances contributing to the widening of the operational areas. The "0" and "1" signals are defined by V_0 and V_1 in that anything less than V_0 is a "0" and anything greater than V_1 is a "1". Unfortunately, these same regions are also the failure mode regions for catastrophic failures.

By use of a linear logic signal system, the transfer characteristics would become similar to Figure 17. There is now a greater amount of signal variation possible, thereby providing higher information content. The decisions which a failure-detection system might make clearly indicate the ease of picking out the logic gates where catastrophic failures have occurred. Linear operation is very costly, however, by reason of the component tolerances required and is particularly bad in the space environment where the peculiarities

12

of that environment, such as radiation and vacuum make tight parameter control very difficult. Future effort on linear logic techniques may, however, produce significant results.

There is another facet to the statement that logic signals should look as unlike the failure mode signals as possible. Where the majority of failures are catastrophic opens or shorts, the use of static logic (d.c. levels) signals invites trouble. The communications practitioner will always endeavor to make his channel signals look as much unlike the anticipated channel noise as possible. If one looks upon the wires from one logic element to another as communications channels, then the same philosophy should apply. It would seem that substantial isolation of catastrophic failures would be gained by a.c. logic signaling systems. Such isolation of elements is necessary in any redundancy scheme in order to prevent a faulty system from totally disabling the decoder which is to correct the fault. By preventing the propagation of the results of a fault over a large portion of the logic system and constraining the area of influence of the failure, the number of failures which a logic system can withstand within itself may be considerably increased without loss of its failure-masking capabilities.

At the present time there are no devices and/or circuits available which exactly fulfill the requirements of failure-erasure circuitry. However, certain of these requirements can be approximated. As an example of existent hardware which, to some extent, has the properties and characteristics outlined above, we would like to consider the parametron.

A parametron element is essentially a resonant circuit with a reactive element varying periodically at frequency 2f which generates a parametric oscillation at the subharmonic frequency f. In practice, the periodic variation is accomplished by applying an exciting current of frequency 2f to a balanced pair of non-linear reactors.

13

A non-linear inductance type was invented in 1954 by Eiichi Goto at Tokyo University.[10] A non-linear capacitance type was suggested by John von Neumann in the United States in 1954.[11] The non-linear inductance type has been widely utilized in Japan as the primary logical element in digital computers. The non-linear capacitance type has been used in the United States with the capacitor a varactor diode.

The subharmonic parametric oscillation generated has the remarkable property in that the oscillation will be stable in either of two phases which differ by π radians with respect to each other. Utilizing this fact, a parametron represents and stores one binary digit, "0" or "1", by the choice between these two phases, 0 or π radians.

If the inductance type circuit shown in Figure 18 is tuned to f, then the output will build up exponentially. The phase of the output will follow the phase of the input which is determined by the algebraic summing action of the coupling transformer at the input. It is this majority vote which allows the device to be utilized as a logical element. A similar description applies to the varactor diode type.

Since oscillation in either of the two stationary states is extremely stable the application of the opposite phase signal at the input during oscillation will have no effect on the parametron. The exciting a.c. signal must be reduced to zero and then increased in order to change the output phase.

Goto has shown that as the resonant circuit of the inductance type parametron is detuned by varying L or C the subharmonic oscillator frequency remains constant but the amplitude changes as shown in Figure 19. Significant detuning in one direction causes the output to go to zero, in the other

---

[10] Goto, E.,"The Parametron, A Digital Computing Element Which Utilizes Parametric Oscillation", Proc. I. R. E., Vol. 47, pp. 1304-1316; August 1959.

[11] A Discussion of von Neumann's original patent application appears in "A New Concept in Computing", R. L. Wigington, Proc. I.R.E. pp. 516-523, April 1959.

direction a tristable region exhibiting hysteresis is encountered. The tri-
stable region has three stable states, 0 phase oscillation, π phase oscillation,
and no oscillation. (It is interesting to note that these three states could
form the basis of a ternary device.) Detuning past this tristate region causes
the output to go to zero.

The parametron fits the specifications for a binary erasure channel "type"
of electronic digital circuit quite well. Given a logical function to perform
the parametron uses a majority vote scheme at its input and then simply ampli-
fies the result. The amplifier is such that changes in its components which
are sufficiently large will cause the output to eventually go to zero. Sim-
ilarly a failure in the input transformer could be disastrous. The channel
model for the parametron could be like that shown in Figure 20. The proba-
bility of going to the correct output state for any input state is p, the
probability of going to the no decision output state from any input state is
q and the probability of going to the incorrect output state from any input
is r (primarily due to the tristate region). The parametron digital circuit
will have $p > q$ and $q > r$. This is a distinct advantage over contemporary
digital circuits in which a "no decision" mode does not exist at all. Because
of the inherent stability of the passive components used r should almost be
zero. The complete circuit to utilize the duplicative redundancy scheme would
be exactly as shown in Figure 12, or Figure 15.

There are also means by which more conventional logic circuitry may be
made amenable to failure-erasure techniques but not without some compromises
on achievable performance.

Let us assume that every logic circuit in a system generates the complement
of its primary output signal. If the failure mode of a circuit is considered
to be the situation where the primary signal of the circuit is identical to
the complementary circuit, then this may be utilized as the single necessary
condition for a "no decision", and error-detection may be accomplished under

the assumed failure-mode condition.

The logic circuit which can fulfill the output requirements is shown in Figure 21. Designed with a view toward development of a universal micro-power logic element, it has two sets of inputs: they are called the AND/NAND input section, and the OR/NOR input section. When the circuit is used as an AND or NAND gate, the standard terms are connected to the AND/NAND input diodes, with the complementary terms connected to the OR/NOR input diodes. The reverse connections are made when the circuit is used for an OR or NOR gate. As an example, let it be assumed that the expression (A X B) is desired. Signal A and signal B are connected individually to diodes D1 and D2, while $\overline{A}$ and $\overline{B}$ are connected to D3 and D4. DeMorgan's theorem and the cross-coupling assure complementary-transistor outputs of operation such that output Y provides the (A X B) term desired and output X the complementary (NAND) term, $(\overline{A \ X \ B})$. In the OR/NOR mode, output X provides the OR term and output Y the NOR term. Although the circuit requires the availability of complementary input signals, it also provides similar output signals for use in subsequent levels of logic.

A flip-flop may be formed by removing point Z from the positive power buss and attaching it to output Y while output X is connected to one of the OR/NOR input diodes.

Circuits of this configuration can display power dissipations of less than 10μ W and switching times less than 0.5μ s, these times being primarily dependent upon input diode capacitance and desired noise immunity.

Using this circuit, the possible sets of output states are:

X	Y	
0	0	failure-mode
0	1	"0"
1	0	"1"
1	1	failure-mode

16

If we now place an MOS field-effect transistor across the circuit as shown in Figure 22, a signal current, I_s, is present only when X = 1 and Y = 0. There is no active response by the FET during failure-mode conditions and at "0" signal because of insufficient biasing signals or complete reverse bias. By utilizing the failure-erasure technique detailed in the paper, the failure-masking configuration of the preceding logic example becomes that shown in Figure 23, where the failure-erasure OR circuit is composed of the two MOS FET's connected together at their drains.

The MOS FET is a desirable circuit element for these configurations because of the large voltage differences required between source and gate before the unit is activated, as well as the exceptionally high input impedances which these transistors display, permitting high degrees of isolation between compared outputs.

It is obvious that an MOS FET failure or a failure of the logic element in its signal state will compromise the system. Variations of this technique can, of course, be applied to the standby-redundancy schemes which require failure detection as an initial procedure before the faulty circuit has its power turned on and the standby unit activated.

CONCLUSIONS

A redundancy technique has been presented which requires mere duplication of elements. In order to bring this technique into practice the circuits used must have certain signaling characteristics. These characteristics have been reviewed and detailed. It is hoped that, in light of the results of this paper, effort will be forthcoming in the areas of device research and circuit design to develop other techniques of realizing failure-erasure circuitry such that future space missions can be made more reliable.

ACKNOWLEDGMENT

(a)
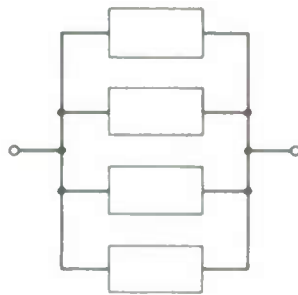
(b)
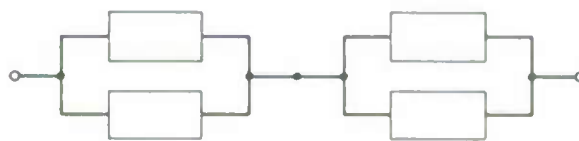
(c)

Fig. 1.   Basic Shannon-Moore Configurations
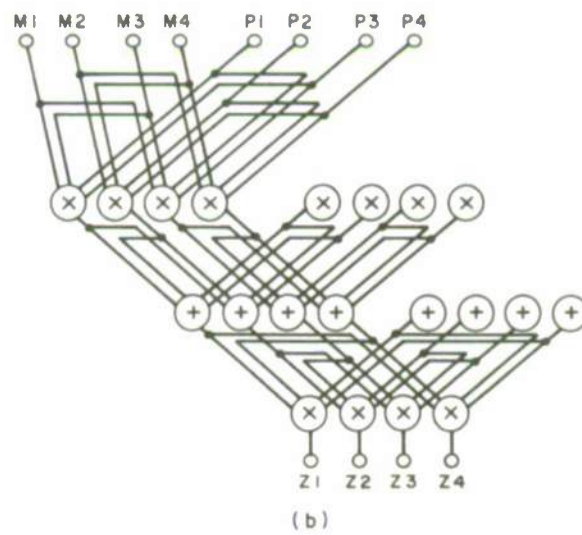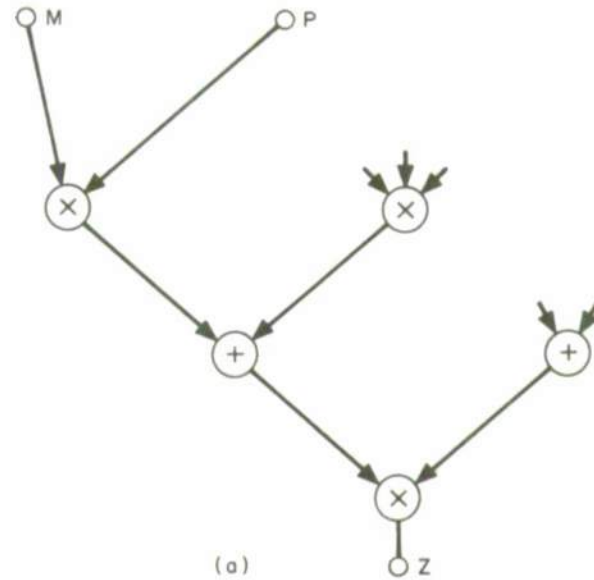
Fig. 2. "Quadded" logic diagram (adapted from Wilcox and Mann, op cit)
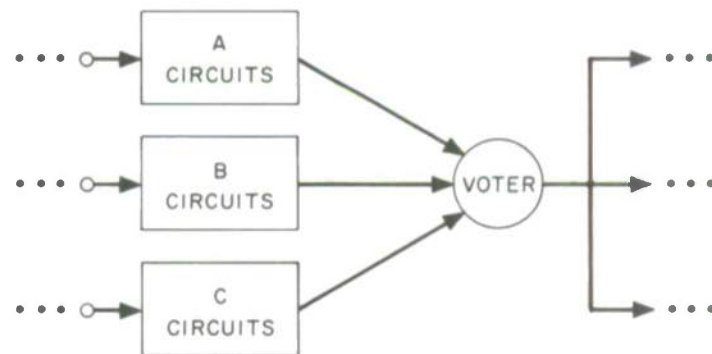
(a)
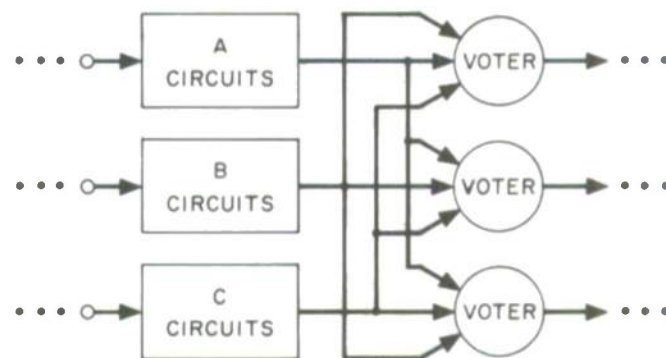
(b)

Fig. 3. Majority voting redundancy configurations
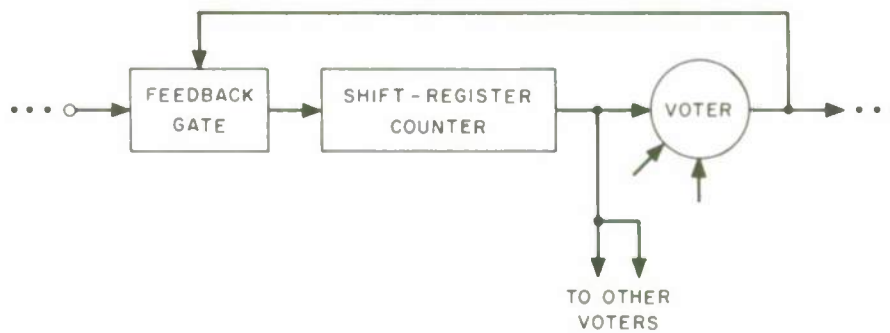
Fig. 4. Transient-failure restoring scheme
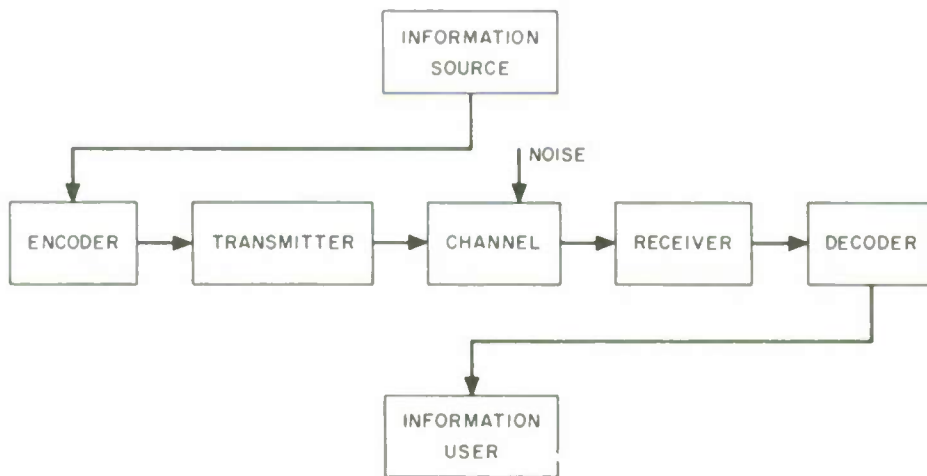
Fig. 5. Block diagram of a digital communication system

3-63-4043
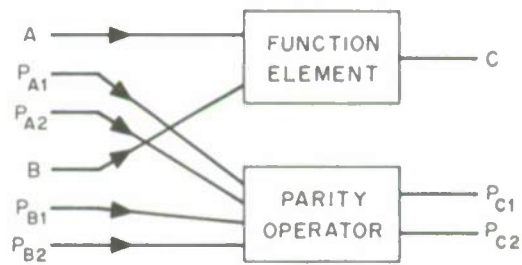
Fig. 6. Communication analog redundant circuit

3-63-4044
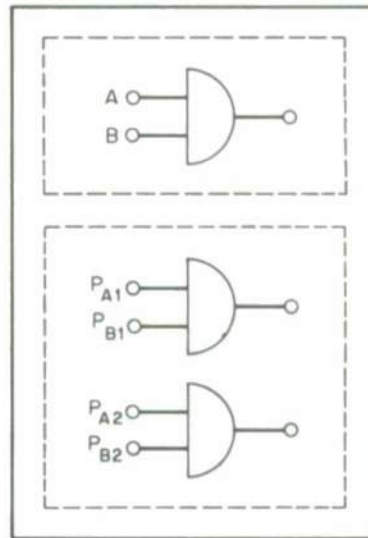
Fig. 7. A hamming code redundant circuit

3-63-4045
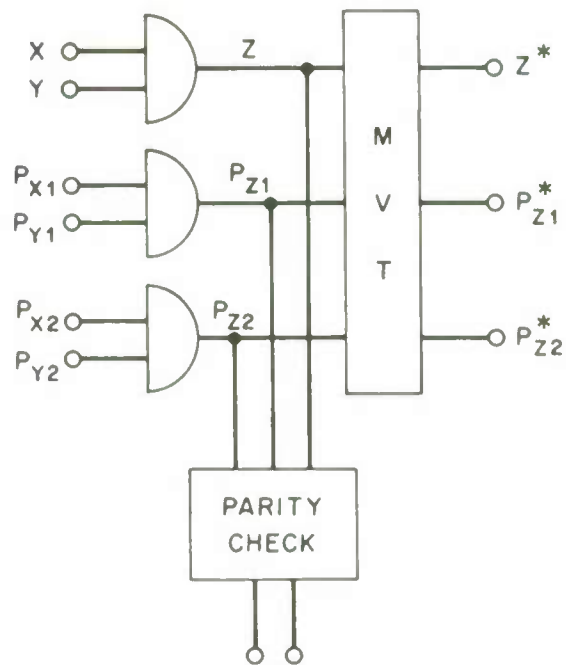
Fig. 8. Optimized decoding

24
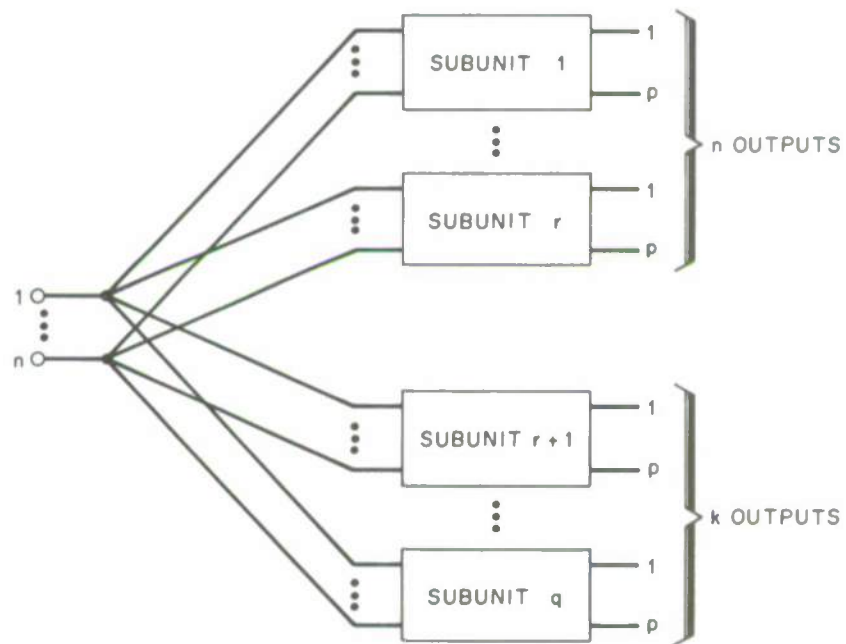
Fig. 9. Sub-unit breakdown
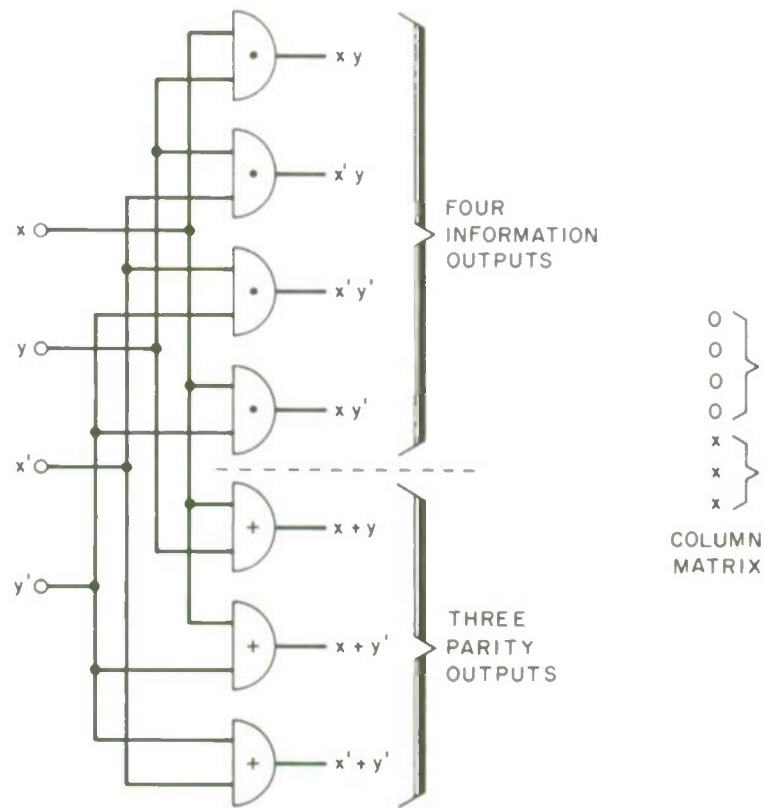
Fig. 10.   Redundant selection circuit
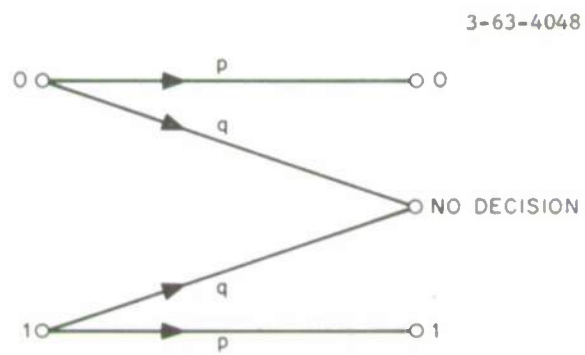
Fig. 11.   Binary erasure channel
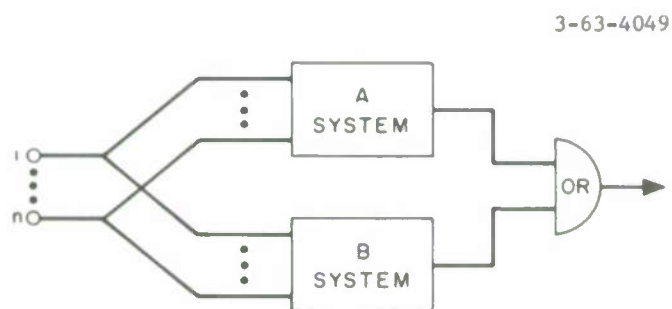
Fig. 12.   Redundant system
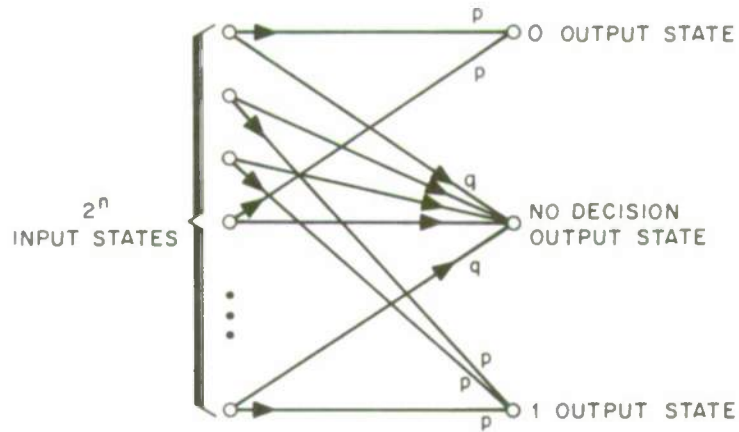
Fig. 13.   A or B system model
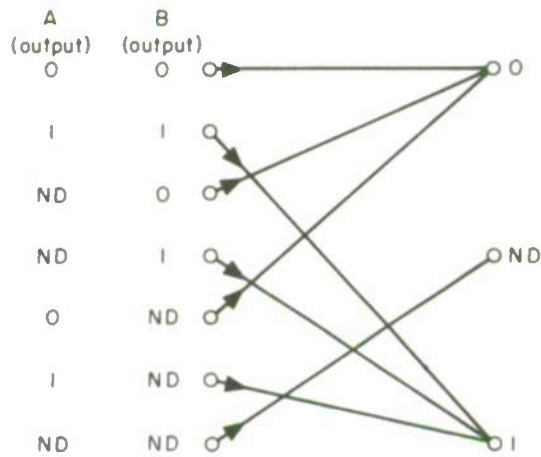
Fig. 14.   Or element operational model

28
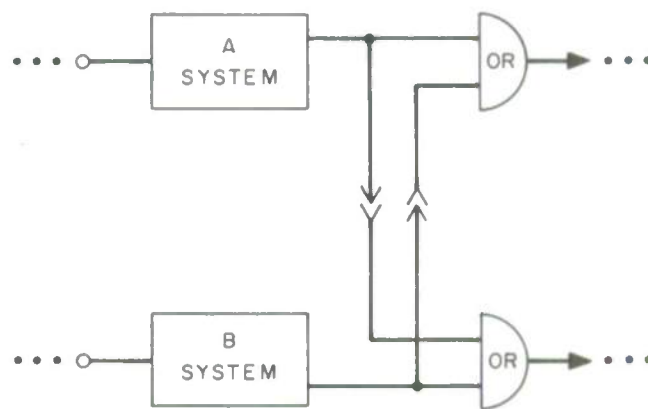
3-63-4052

Fig. 15. Complete system diagram
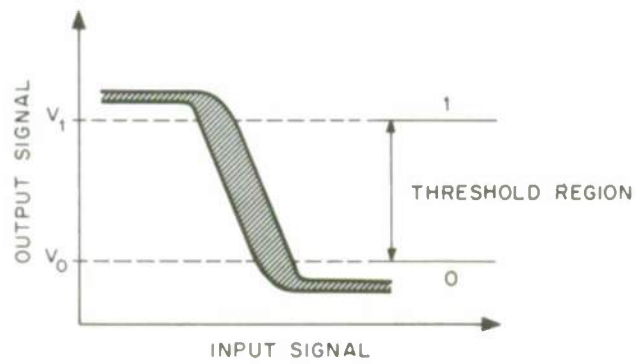
Fig. 16.   Typical digital transfer characteristic
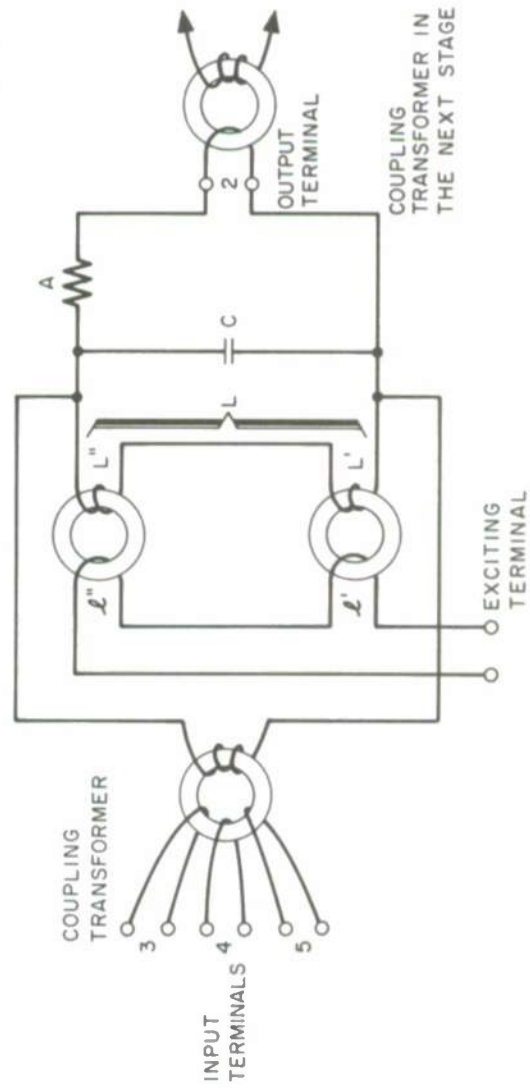
Fig. 17.   Linear system transfer characteristic

3-63-4055

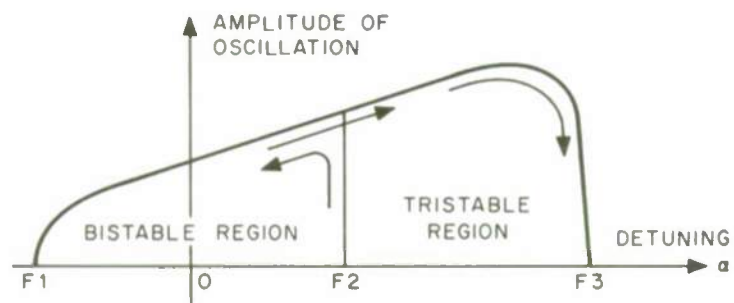Fig. 18. Parametron as a logic element (adapted from Ref. 10)

31

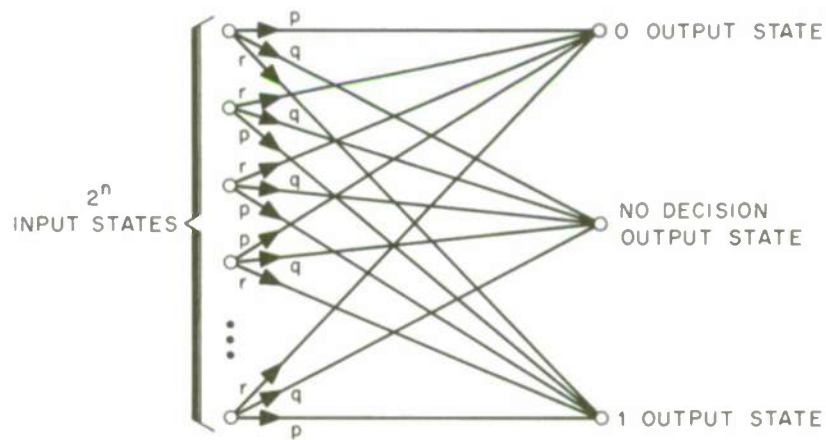Fig. 19.   Stability profile (from Ref. 10)
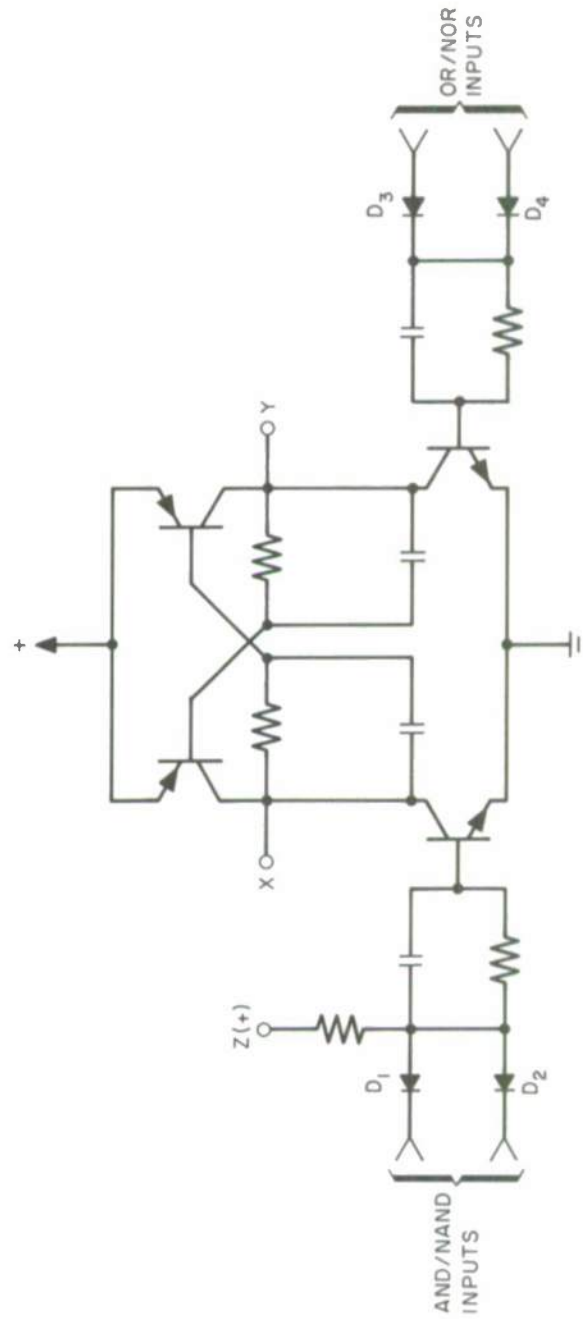
Fig. 20.   Channel analog for parametron
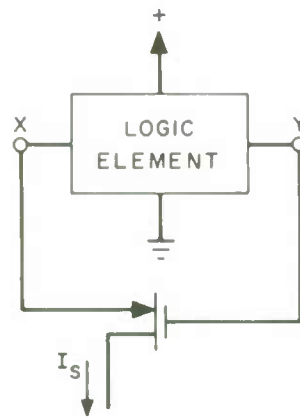
Fig. 21. Universal micropower logic element

3-63-4059
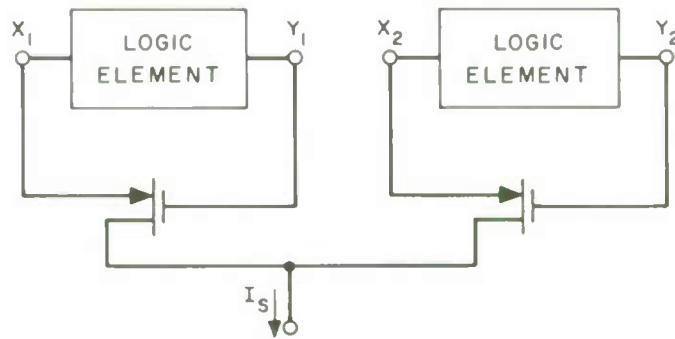

Fig. 22.   Failure-erasure logic element

3-63-4060

Fig. 23.   Failure masking logic element

34

DISTRIBUTION LIST

Division 6

G. P. Dinneen

E. W. Morrow, Jr.

Group 62

Y. Cho

Group 63

M. Ash

G. H. Ashley

R. S. Berg

J. Binsack

W. L. Black

A. Braga-Illa

C. Burrowes

R. Chick

N. B. Childs

M. C. Crocker

J. B. Connolly

F. W. Floyd

A. I. Grayzel

B. Howland

R. M. Lerner

C. L. Mack

D. C. MacLellan

J. Max

J. D. McCarron

R. E. McMahon

L. Michelove

B. J. Moriarty

D. Nathanson

D. Parker

J. Ryan

F. W. Sarles

W. Schmidt

V. Sferrino

I. Shapiro

H. Sherman

R. L. Sicotte

W. B. Smith

D. M. Snider

A. Stanley

D. Tang

L. J. Travis

N. Trudeau

E. Vrablik

P. Waldron

Group 66

B. Reiffen

B. E. White

Group 63 Files
10 copies

35

DOCUMENT CONTROL DATA - R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author)	2a. REPORT SECURITY CLASSIFICATION
Lincoln Laboratory, M.I.T.	Unclassified
	2b. GROUP None

3. REPORT TITLE

Failure Erasure Circuitry: A Duplicate Technique for Failure-Masking Systems

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

Technical Note

5. AUTHOR(S) *(Last name, first name, initial)*

Connolly, John B. and Schmidt, William G.

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
14 October 1965	42	11

6a. CONTRACT OR GRANT NO. AF 19(628)-5167	9a. ORIGINATOR'S REPORT NUMBER(S)
b. PROJECT NO. 649L	Technical Note 1965-3
c.	9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
d.	ESD-TDR-65-555

10. AVAILABILITY/LIMITATION NOTICES

None

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
None	Air Force Systems Command, USAF

13. ABSTRACT

The purpose of this paper is to describe a redundancy technique which would require mere duplication to achieve the same failure-masking capabilities as von Neumann's triplication and majority-voting technique.

An analysis of the circuit-failure problem is approached from the viewpoint of coding theory with comparisons made between the "noisy channel" and "circuit-failure" problems. Some of the difficulties of extrapolating from the former to the latter are discussed, as well as recent attempts to minimize the redundancy "overhead" by coding over larger numbers of bits.

Following a description of the binary erasure channel model, a proposal of a failure-erasure technique based upon it is outlined. The method enables failure-masking at duplicative rather than triplicative costs. There are constraints which this scheme imposes upon the circuit elements, however, and the characteristics of the ideal circuit element and logic signaling are proposed. The paper concludes with a discussion of existing hardware which approximates the desired characteristics.

14. KEY WORDS

circuit failure
coding theory
noise

failure-masking system
binary erasure

redundancy
digital systems